CE441: Data and Network Security

Cyber Security: Problem Overview

Behnam Momeni, PhD

Department of Computer Engineering
Sharif University of Technology

Fall 2019
Outline

1. What Does Security Mean?
   - Model and Definition
     - Game-based Definition
     - Simulation-based Definition

2. Security Life-Cycle

3. Security/Insecurity Incentives
What Does It Mean to be Secure?

- **Intuitively,**
  - to provide some functionality
  - without being misused for other purposes
    - e.g. to open an email attachment without installing a malware
    - or to serve a webpage without allowing users to modify it

- **Precisely,**
  - it depends on the context,
  - can be modeled (i.e. which operations are acceptable?),
  - and should be defined (i.e. a formal statement to be proved)

*Let’s go precise...*
What Does It Mean to be Secure?

- **Intuitively,**
  - to provide **some functionality**
  - without being **misused** for other purposes
    - *e.g.* to open an email attachment **without** installing a malware
    - *or* to serve a webpage **without** allowing users to modify it

- **Precisely,**
  - it depends on the **context,**
  - can be **modeled** (*i.e.* which operations are acceptable?),
  - and should be **defined** (*i.e.* a formal statement to be proved)

- *Let’s go precise...*
Security Goals

CIA Triad

- Availability
- Confidentiality
- Integrity
Model

- **Model** is a depiction of reality *without inappropriate details*
  - It might be smaller in size → *Maquette of a building*
  - or omit some aspects → *A software prototype*
  - or be more *abstract* (conceptually) → *A sphere instead of a planet*
- Focused on the interesting aspects and details to be studied

**Adversarial Model**

- Which operations can be carried on by an adversary.
  - e.g. Can intercept and modify network packets
Model

- **Model** is a depiction of reality *without inappropriate details*
  - It might be smaller in size → *Maquette of a building*
  - or omit some aspects → *A software prototype*
  - or be more *abstract* (conceptually) → *A sphere instead of a planet*
- Focused on the interesting aspects and details to be studied

### Adversarial Model

- Which operations can be carried on by an adversary.
  - *e.g.* Can intercept and modify network packets
Definition

Defining an **scheme** has two main parts

- **Syntax**: specifies operations which can be performed by honest participants of the scheme
  - *e.g.* The symmetric encryption scheme, $SE = (K, E, D)$, contains a key generation function $K$, an encryption function $E$, and a decryption function $D$
  - $k \leftarrow K : \forall m . \ D_k(E_k(m)) = m$
  - The scheme is **modeled** here

- **Semantic**: specifies conditions which must be met by a **secure** scheme
  - The **security definition** is formalized here
Outline

1. What Does Security Mean?
   - Model and Definition
   - Game-based Definition
   - Simulation-based Definition

2. Security Life-Cycle

3. Security/Insecurity Incentives
Game-based Definition

- Model the scheme operations normally
- Then, devise a game between an adversary and a challenger
  - Adversary tries to break the security definition
  - Challenger wants to demonstrate inability of the adversary
- Adversary is trying to obtain some advantage
  - e.g. in an encryption scheme, an adversary might want to learn the key or she might want to decrypt a ciphertext
  - The advantage of an adversary can be defined in terms of a success probability
    - How probable is it to guess the key correctly?
    - As probable as a random guess? → No advantage
    - Better than a random guess? → Scheme is not too strong
- Formalize the advantage
What Does Security Mean?

Game-based Definition

Model the scheme operations normally

Then, devise a game between an adversary and a challenger

- Adversary tries to break the security definition
- Challenger wants to demonstrate inability of the adversary

Adversary is trying to obtain some advantage

- e.g. in an encryption scheme, an adversary might want to learn the key or she might want to decrypt a ciphertext
- The advantage of an adversary can be defined in terms of a success probability

  - How probable is it to guess the key correctly?
  - As probable as a random guess? → No advantage
  - Better than a random guess? → Scheme is not too strong

Formalize the advantage
Game-based Definition

- Model the scheme operations normally
- Then, devise a game between an adversary and a challenger
  - Adversary tries to break the security definition
  - Challenger wants to demonstrate inability of the adversary
- Adversary is trying to obtain some advantage
  - e.g. in an encryption scheme, an adversary might want to learn the key or she might want to decrypt a ciphertext
  - The advantage of an adversary can be defined in terms of a success probability
    - *How probable is it to guess the key correctly?*
    - *As probable as a random guess?* → No advantage
    - *Better than a random guess?* → Scheme is not too strong
- Formalize the advantage
What Does Security Mean?

Game-based Definition

IND-CPA – Game-based Definition

- For example, consider the scheme of \( S\mathcal{E} = (\mathcal{K}, \mathcal{E}, \mathcal{D}) \)
- The game of **ciphertext indistinguishability** under the chosen plaintext attack (IND-CPA) is defined as follows:
  - **Challenger** generates a secret key and a random \( b \) from \( \{0, 1\} \)
    - \( k \xleftarrow{\$} \mathcal{K}, b \xleftarrow{\$} \{0, 1\} \)
  - **Adversary** selects two possible messages: \( M_0 \) and \( M_1 \)
  - **Challenger** encrypts \( M_b \) and reveals \( C_b \xleftarrow{\$} \mathcal{E}_k(M_b) \)
  - **Adversary** must guess the \( b \) and distinguish \( C_0 \) from \( C_1 \)
  - **Adversary** can ask about encryption of any plaintext

- The advantage of an adversary (\( A \)) can be formalized as
  - \( \text{Adv}_{SE}(A) = 2\mathbb{P}[\text{Guess}_{SE}(A) = \text{true}] - 1 \)
- Scheme is defined to be secure if and only if
  - \( \text{Adv}_{SE}(A) \) is negligible for all \( A \)
  - Abilities of \( A \) can be restricted by a model
IND-CPA – Game-based Definition

- For example, consider the scheme of $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
- The game of *ciphertext indistinguishability* under the *chosen plaintext attack* (IND-CPA) is defined as follows:
  - **Challenger** generates a secret key and a random $b$ from $\{0, 1\}$
    - $k \leftarrow \mathcal{K}$, $b \leftarrow \{0, 1\}$
  - **Adversary** selects two possible messages: $M_0$ and $M_1$
  - **Challenger** encrypts $M_b$ and reveals $C_b \leftarrow \mathcal{E}_k(M_b)$
  - **Adversary** must guess the $b$ and distinguish $C_0$ from $C_1$
  - **Adversary** can ask about encryption of any plaintext
- The advantage of an adversary ($A$) can be formalized as
  - $\text{Adv}_{\mathcal{SE}}(A) = 2\mathbb{P}[\text{Guess}_{\mathcal{SE}}(A) = \text{true}] - 1$
- Scheme is defined to be secure if and only if
  - $\text{Adv}_{\mathcal{SE}}(A)$ is negligible for all $A$
  - Abilities of $A$ can be restricted by a model
IND-CPA – Game-based Definition

- For example, consider the scheme of $\mathcal{S} \mathcal{E} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
- The game of **ciphertext indistinguishability** under the **chosen plaintext attack** (IND-CPA) is defined as follows:
  - **Challenger** generates a secret key and a random $b$ from $\{0, 1\}$
    - $k \xleftarrow{\$} \mathcal{K}, b \xleftarrow{\$} \{0, 1\}$
  - **Adversary** selects two possible messages: $M_0$ and $M_1$
  - **Challenger** encrypts $M_b$ and reveals $C_b \xleftarrow{\$} \mathcal{E}_k(M_b)$
  - **Adversary** must guess the $b$ and distinguish $C_0$ from $C_1$
  - **Adversary** can ask about encryption of any plaintext
- The advantage of an adversary ($A$) can be formalized as
  - $\text{Adv}_{\mathcal{S} \mathcal{E}}(A) = 2\mathbb{P}[\text{Guess}_{\mathcal{S} \mathcal{E}}(A) = \text{true}] - 1$
- Scheme is defined to be secure if and only if
  - $\text{Adv}_{\mathcal{S} \mathcal{E}}(A)$ is negligible for all $A$
  - Abilities of $A$ can be restricted by a model
Outline

1. What Does Security Mean?
   - Model and Definition
   - Game-based Definition
   - Simulation-based Definition

2. Security Life-Cycle

3. Security/Insecurity Incentives
Simulation-based Definition

- Consider an **ideal** world parallel to the **real** world
  - The scheme is defined similarly in both worlds
  - But the **ideal** world is modified slightly to be trivially secure
- The **real** world’s security can be defined based on the **ideal** world
  - Build an algorithm \( S \) which works in the **ideal** world and simulates the behavior of an adversary \( A \) which works in the **real** world
  - If such a simulator exists for all adversaries, then both words will be semantically equivalent (*Why?*)
  - Equivalence of both worlds means that the **real** world is as secure as the **ideal** world which was trivially secure
  - Scheme is defined to be secure if and only if such a simulator exists
Simulation-based Definition

- Consider an **ideal** world parallel to the **real** world
  - The scheme is defined similarly in both worlds
  - But the **ideal** world is modified slightly to be trivially secure
- The **real** world’s security can be defined based on the **ideal** world
  - Build an algorithm $S$ which works in the **ideal** world and simulates the behavior of an adversary $A$ which works in the **real** world
  - If such a simulator exists for all adversaries, then both words will be semantically equivalent (*Why?*)
  - Equivalence of both worlds means that the **real** world is as secure as the **ideal** world which was trivially secure
  - Scheme is defined to be secure if and only if such a simulator exists
IND-CPA – Simulation-based Definition

- For example, consider the scheme of $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$
- In the real world, an adversary $A$ had access to the encryption of $M_b$ and had to guess the value of $b$
- In the ideal world, the encryption of $M_b$ is not provided and hence no knowledge about $b$ might be extracted from it
- Scheme is secure if a simulator $S$ can be built in the ideal world to simulate the output distribution of $A$ from the real world
- A simplified definition for the advantage of adversary is
  - $b \leftarrow \{0, 1\}$, $k \leftarrow \mathcal{K}$, $C_b \leftarrow \mathcal{E}_k(M_b)$
  - $\text{Adv}_{\mathcal{SE}}(A) = P[A(1|C_b|, C_b, 1|M_b|) = b] - P[S(1|C_b|, 1|M_b|) = b]$
  - For the complete definition check [simproof]
- If scheme is secure, there will be an $S$ for each $A$ which makes $\text{Adv}_{\mathcal{SE}}(A)$ negligibly small
IND-CPA – Simulation-based Definition

For example, consider the scheme of $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$

In the real world, an adversary $A$ had access to the encryption of $M_b$ and had to guess the value of $b$

In the ideal world, the encryption of $M_b$ is not provided and hence no knowledge about $b$ might be extracted from it

Scheme is secure if a simulator $S$ can be built in the ideal world to simulate the output distribution of $A$ from the real world

A simplified definition for the advantage of adversary is

- $b \xleftarrow{\$} \{0, 1\}, \ k \xleftarrow{\$} \mathcal{K}, \ C_b \xleftarrow{\$} \mathcal{E}_k(M_b)$
- $\text{Adv}_{\mathcal{SE}}(A) = \mathbb{P}[A(1|C_b|, C_b, 1|M_b|) = b] - \mathbb{P}[S(1|C_b|, 1|M_b|) = b]$
  - For the complete definition check [simproof]

If scheme is secure, there will be an $S$ for each $A$ which makes $\text{Adv}_{\mathcal{SE}}(A)$ negligibly small
Outline

1. What Does Security Mean?
2. Security Life-Cycle
   - System Development
   - Creative Attack Examples
3. Security/Insecurity Incentives
Developing a Secure System – Preliminaries

Risk → Threat → Attack → Exploit

Impact → Vulnerability
Developing a Secure System – Preliminaries

Risk -> Threat -> Attack

Impact -> Vulnerability -> Exploit
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling
4. Defining Security & Formal Proofs (Optional)
5. System Design
6. Implementation & Test
7. Deployment Operation & Maintenance
Security Life-Cycle – Threat Analysis

- Range of threats
  - from script kiddies to state-level attackers
  - insiders
  - cyber-warfare

- Why does it matter?
  - Security Economics
    - cost-of-security ≤ cost-of-damage ≤ system-value
  - A shop selling 1$ snacks protected by a 100$ CCTV camera system!
Security Life-Cycle – Threat Analysis

- Range of threats
  - from script kiddies to state-level attackers
  - insiders
  - cyber-warfare

- Why does it matter?
  - Security Economics
    - cost-of-security $\leq$ cost-of-damage $\leq$ system-value
  - A shop selling 1$ snacks protected by a 100$ CCTV camera system!
Be Realistic About Modeling Threats...

[A Crypto Nerd’s Imagination: His laptop’s encrypted. Let’s build a million-dollar cluster to crack it.

No good! It’s 4096-bit RSA! Blast! Our evil plan is foiled!]

[What would actually happen: His laptop’s encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.]
Security Life-Cycle – Policy Specification

- A high level document specifying
  1. Management goals/objectives to secure the assets
  2. Security threats, damage impacts, and risks
  3. Responsibilities of each party to manage the identified risks and corresponding procedures and guidelines
  4. Standards and technologies which should be complied/used

- e.g. To access Internet through the university network, students shall be authenticated and authorized independently

- e.g. Network users are not allowed to monitor the network traffic of other users
Developing a Secure System – Life-Cycle

1. Threat Analysis

2. Policy Specification

B. Momeni (Sharif Univ. of Tech.)
CE441: Data and Network Security
Fall 2019 19/44
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling

B. Momeni (Sharif Univ. of Tech.)
CE441: Data and Network Security
Fall 2019
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling
4. Defining Security & Formal Proofs (Optional)
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling
4. Defining Security & Formal Proofs (Optional)
5. System Design
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling
4. Defining Security & Formal Proofs (Optional)
5. System Design
6. Implementation & Test
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling
4. Defining Security & Formal Proofs (Optional)
5. System Design
6. Implementation & Test
7. Deployment Operation & Maintenance
Developing a Secure System – Life-Cycle

1. Threat Analysis
2. Policy Specification
3. Security Modeling
4. Defining Security & Formal Proofs (Optional)
5. System Design
6. Implementation & Test
7. Deployment Operation & Maintenance

B. Momeni (Sharif Univ. of Tech.)
CE441: Data and Network Security
Fall 2019
Outline

1. What Does Security Mean?
2. Security Life-Cycle
   - System Development
   - Creative Attack Examples
3. Security/Insecurity Incentives
Creative Attack Examples – Confidentiality

- Eavesdropping – undermining data confidentiality
  - Can be mitigated by cryptography
  - But the message length might be leaked yet

- Traffic Analysis
  - Stories of the “Pentagon Pizza Deliveries,” “El Chapo’s Capture,” etc.

Ref [left]: https://www.washingtonpost.com/wp-srv/national/images/pizza_121898r.jpg
Ref [right]: https://www.washingtonpost.com/wp-srv/national/images/pizza_121898.gif
Creative attacks!

- Can I find out what links you have visited?
  - Use javascript to get the color of the links on the page
  - Can find out if you have visited a specific link (This was fixed)!
  - Set the background color to that of the visited link color, and employ Captchas

\[
\begin{align*}
4 + 5 &= 9; \\
4 + F &= A; \\
5 + F &= 6; \\
4 + 5 + F &= 8
\end{align*}
\]

Borrowed from [40442-971:00-pre-intro.pdf], page 12
Creative Attack Examples – Integrity

- Phishing – undermining integrity of the website/email sender’s identity (i.e. authenticity)
- A fake website similar to the original website
- Or an email to convince people to reveal their valuable information
Phishing Email Targeting Berkeley Students

From: <NAME REMOVED>
Date: Sat, Apr 1, 2017 at 2:09 PM
Subject: Library Account
To: xxxxx@berkeley.edu

Dear Student,

Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account. For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile.

https://auth.berkeley.edu/cas/login?service=https%3a%2f

If you are not able to login, please contact <Name Removed> at xxxxx@berkeley.edu for immediate assistance.

Sincerely,

<Name Removed>
University Library
University of California Berkeley

Ref: https://security.berkeley.edu/news/phishing-example-library-account-0
Creative Attack Examples – Availability

- Distributed Denial of Service (DDoS) – undermining availability
- An attack with 1.35 Tbps against GitHub
  - An amplification attack using the memcached (UDP port 11211)
  - 17:21 UTC February 28, 2018

Ref: https://github.blog/2018-03-01-ddos-incident-report/
Insider attacks: example

Hidden trap door in Linux (nov 2003)
– Allows attacker to take over a computer
– Practically undetectable change (uncovered via CVS logs)

Inserted line in wait4()

```c
if (((options == (__WCLONE|__WALL)) && (current->uid = 0))
    retval = -EINVAL;
```  

Looks like a standard error check, but ...

See: http://lwn.net/Articles/57135/

Dan Boneh
Outline

1. What Does Security Mean?
2. Security Life-Cycle
3. Security/Insecurity Incentives
   - Dark Market Value
   - Bug Bounty Programs
   - Security vs. X Trade-off
Dark Market Value

- There are underground markets for cyber-criminal activities
  - *e.g.* check [undrgrnd101](#) about Russian underground markets
    - ANTICHAT.ru
    - xeka.ru
    - Exploit.IN
    - XaKePoK.su
    - ...

- Different vulnerability exploitation services, dedicated machine renting, malware installation services, distributed denial of service, etc. are sold

- An example post about the ZeuS botnet (translated from Russian):
### Dark Market Value – Pay Per Install

<table>
<thead>
<tr>
<th>Offering</th>
<th>Price per 1,000 Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia (AU)</td>
<td>US$300-550</td>
</tr>
<tr>
<td>Great Britain (UK)</td>
<td>US$220-300</td>
</tr>
<tr>
<td>Italy (IT)</td>
<td>US$200-350</td>
</tr>
<tr>
<td>New Zealand (NZ)</td>
<td>US$200-250</td>
</tr>
<tr>
<td>Spain (ES), Germany (DE), or France (FR)</td>
<td>US$170-250</td>
</tr>
<tr>
<td>United States (US)</td>
<td>US$100-150</td>
</tr>
<tr>
<td>Global mix</td>
<td>US$12-15</td>
</tr>
<tr>
<td>European mix</td>
<td>US$80</td>
</tr>
<tr>
<td>Russia (RU)</td>
<td>US$100</td>
</tr>
</tbody>
</table>

*Table 4: PPI service prices*

### Dark Market Value – DDoS Service

<table>
<thead>
<tr>
<th>Offering</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-day DDoS service</td>
<td>US$30-70</td>
</tr>
<tr>
<td>1-hour DDoS service</td>
<td>US$10</td>
</tr>
<tr>
<td>1-week DDoS service</td>
<td>US$150</td>
</tr>
<tr>
<td>1-month DDoS service</td>
<td>US$1,200</td>
</tr>
</tbody>
</table>

*Table 5: DDoS service prices*

Other Incentives for Insecurity – NSA

  - Vulnerability was kept secret, so vulnerable systems could be exploited

- The Shadow Brokers hacking group gains access to the developed exploits including the Eternal Blue vulnerability, publishes some files for free, and starts an auction to sell the rest in 2016 (Ref: ArsTechnica-2016/08/16-group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof)

- NSA reports to Microsoft about the vulnerability in 2017 (CVE-2017-0144)

- The WannaCry ransomware outbreak started (in 2017) using the Eternal Blue vulnerability, encrypting files and asking for a ransom to decrypt them
  - e.g. it hit UK hospitals hard, with multiple sources reporting closures of entire wards, patients being turned away and ... (Ref: Forbes-2017/05/12-nsa-exploit-used-by-wannacry-ransomware-in-global-explosion)
Other Incentives for Insecurity – NSA

  - Vulnerability was kept secret, so vulnerable systems could be exploited

- The Shadow Brokers hacking group gains access to the developed exploits including the Eternal Blue vulnerability, publishes some files for free, and starts an auction to sell the rest in 2016 (Ref: ArsTechnica-2016/08/16-group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof)

- NSA reports to Microsoft about the vulnerability in 2017 (CVE-2017-0144)
  - The WannaCry ransomware outbreak started (in 2017) using the Eternal Blue vulnerability, encrypting files and asking for a ransom to decrypt them
  - e.g. it hit UK hospitals hard, with multiple sources reporting closures of entire wards, patients being turned away and ... (Ref: Forbes-2017/05/12-nsa-exploit-used-by-wannacry-ransomware-in-global-explosion)
Other Incentives for Insecurity – NSA

  - Vulnerability was kept secret, so vulnerable systems could be exploited

- The Shadow Brokers hacking group gains access to the developed exploits including the Eternal Blue vulnerability, publishes some files for free, and starts an auction to sell the rest in 2016 (Ref: ArsTechnica-2016/08/16-group-claims-to-hack-nsa-tied-hackers-posts-exploits-as-proof)

- NSA reports to Microsoft about the vulnerability in 2017 (CVE-2017-0144)

- The WannaCry ransomware outbreak started (in 2017) using the Eternal Blue vulnerability, encrypting files and asking for a ransom to decrypt them
  - e.g. it hit UK hospitals hard, with multiple sources reporting closures of entire wards, patients being turned away and ... (Ref: Forbes-2017/05/12-nsa-exploit-used-by-wannacry-ransomware-in-global-explosion)
Eternal Blue – WannaCry Ransomware

Kafeine
@kafeine

WannaCry/WanaCrypt0r 2.0 is indeed triggering ET rule : 2024218 "ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"

Ref: https://twitter.com/kafeine/status/863049739583016960

8:14 AM - 12 May 2017
Why own machines:
1. IP address and bandwidth stealing

Attacker’s goal: look like a random Internet user

Use the IP address of infected machine or phone for:

• **Spam**  (e.g. the storm botnet)
  Spamalytics: 1:12M pharma spams leads to purchase
  1:260K greeting card spams leads to infection

• **Denial of Service**: Services: 1 hour (20$), 24 hours (100$)

• **Click fraud**  (e.g. Clickbot.a)

Dan Boneh

Borrowed from [40442-971:01-intro.pdf], page 7
Why own machines:

2. Steal user credentials and inject ads
keylog for banking passwords, web passwords, gaming pwds.

Example: SilentBanker (and many like it)
Users attacked: stats

≈ 300,000 users worldwide

A worldwide problem


Borrowed from [40442-971:01-intro.pdf], page 10
Why own machines:  

3. Ransomware

<table>
<thead>
<tr>
<th>Rank</th>
<th>Malware Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Trojan-Ransom.HTML.Agent</td>
</tr>
<tr>
<td>2</td>
<td>Trojan-Ransom.JS.Blocker</td>
</tr>
<tr>
<td>3</td>
<td>Trojan-Ransom.JS.InstallExtension</td>
</tr>
<tr>
<td>4</td>
<td>Trojan-Ransom.NSIS.Onion</td>
</tr>
<tr>
<td>5</td>
<td>Trojan-Ransom.Win32.Cryakl</td>
</tr>
<tr>
<td>6</td>
<td>Trojan-Ransom.Win32.Cryptodef</td>
</tr>
<tr>
<td>7</td>
<td>Trojan-Ransom.Win32.Snochry</td>
</tr>
<tr>
<td>8</td>
<td>Trojan-Ransom.BAT.Scatter</td>
</tr>
<tr>
<td>9</td>
<td>Trojan-Ransom.Win32.Crymod</td>
</tr>
<tr>
<td>10</td>
<td>Trojan-Ransom.Win32.Shade</td>
</tr>
</tbody>
</table>

CryptoWall (2014-)
- targets Windows
- spread by spam emails

≈ 200,000 machines in 2015
A worldwide problem.

Dan Boneh
Why own machines:

4. Spread to isolated systems

Example: Stuxnet

Windows infection \Rightarrow

Siemens PCS 7 SCADA control software on Windows \Rightarrow

Siemens device controller on isolated network

More on this later in course

Borrowed from [40442-971:01-intro.pdf], page 12
Outline

1. What Does Security Mean?
2. Security Life-Cycle
3. Security/Insecurity Incentives
   - Dark Market Value
   - Bug Bounty Programs
   - Security vs. X Trade-off
Bug Bounty Programs – Direct

- Some vendors encourage security researchers to find and report vulnerabilities in order to make their products and services more secure.

- **Google** Vulnerability Reward Program (VRP)
  - *.google.com, *.youtube.com, *.blogger.com (Ref: [https://www.google.com/about/appsecurity/reward-program/](https://www.google.com/about/appsecurity/reward-program/))
  - Rewards for qualifying bugs range from $100 to $31,337.

- **Mozilla** Security Bug Bounty Program
Bug Bounty Programs – Indirect

- Some programs encourage researchers on behalf of the vendors to find their vulnerabilities in order to
  - Use vulnerabilities in their security tools (e.g. IPS)
  - Report vulnerabilities to vendors as a proxy

- e.g. Zero Day Initiative (Ref: https://www.zerodayinitiative.com/about/benefits/)
Outline

1. What Does Security Mean?
2. Security Life-Cycle
3. Security/Insecurity Incentives
   - Dark Market Value
   - Bug Bounty Programs
   - Security vs. X Trade-off
Security vs. Usability

- A firewall which asks for user intervention continuously
- An intrusion detection system which shows ten alarms per second filled by false-positives
Security vs. Performance

- Runtime overhead for encrypting/decrypting data increases when the key size used and the number of encryption rounds increase.
- Low quality pseudo-random numbers are generated fast:
  - *e.g.* `rand()` in C
- While high quality random numbers take longer to be generated:
  - *e.g.* `getrandom()` in C
- And even in the information theory:
  - A Computationally Unbounded Adversary
  - A Probabilistic Polynomial Time (PPT) Adversary
Security vs. Development Cost

- Allocating extra time to develop securely
  → More Cost

- Requiring less time to fix the missed bugs in the late phases
  → Less Cost
  - Least costly solution is to manage security as a proactive process
  - Integrated in the development life-cycle

- Value of the system which is being developed vs. Its development cost

- Risk of a vulnerability
  - How probable is it to be exploited?
  - What is its impact if exploited successfully?

- Address issues based on their risk amounts
References and Further Reading


- [phish] “Phishing | Information Security Office,” Berkeley University of California, Online: https://security.berkeley.edu/education-awareness/phishing/, 2019
