NETWORK SECURITY PRACTICES

ATTACK AND DEFENSE

Yusung Wu

Overview

- The course focuses on the discussion of system-level security issues and their defenses
- Prerequisites
  - Knowledge of operating systems and computer networks, C programming,…
- Grading
  - Project 70%
  - Final Exam 30%

Syllabus

主題	子議題	Project
Introduction		Malware and exploit collection
Vulnerabilities and Exploits	Malware	
	Vulnerabilities	
	Exploits	On-access virus scanner
Crypto. Primitives	Symmetric and Asymmetric Crypto	
	Hash and MAC	
	Key Agreement and Forward Secrecy	Key derivation
Network Security	Routing	
	Resource lookup	
	Content	Using OpenSSL in network programming
	PKI	
	Reconnaissance	
	Anonymity and Privacy	Anonymous Network
	DDoS	
Host Security	Access Control Models	
	UNIX	OAuth 2.0 Authorization Framework
	Windows	
	SELinux	
Code Injection	SQL Injection	
	Buffer Overflow	
Web Security	Web Security Model	
	CORS, XSS, CSRF	
Cloud Computing Security	Virtualization	
	Mobile Device Management	

What is security about?

- Cryptography ?
- Virus ?
- Hacker ?
- …?

What is security about?

- Confidentiality
  - Hide data and resource
- Integrity
  - Data Integrity
  - Origin Integrity (authentication)
- Availability
  - Access to data and resources

Why do we care about the CIA?

- Privacy
  - The ability to keep some things to yourself
- Anonymity
  - When you want people to see what you do, just not that it's you doing it
- Authenticity
  - You want people to know, *for sure*, it is you, who are doing the thing
- Accountability
  - The ability to know who did what

Two million stolen Facebook, Twitter, Yahoo, ADP passwords found on Pony Botnet server

Summary: *Trustwave's SpiderLabs found a Pony Botnet Controller server holding over two million passwords and account credentials for ADP payroll, Facebook, Twitter, Yahoo and more belonging to victims around the world.*

By Violet Blue for Zero Day | December 4, 2013 -- 10:02 GMT (18:02 SGT)

Follow @violetblue Get the ZDNet Security newsletter now

Since the source code for the Pony Botnet Controller was leaked, Trustwave's SpiderLabs has been tracking the beast with much fascination.

Interest turned to stunned surprise when the researchers uncovered a Pony Botnet server stabling over two million account credentials and passwords for Facebook, Yahoo, Google, Twitter, Linkedin, Odnoklassniki (the second largest Russian social network site) and more.

Contrary to what some news outlets are reporting, SpiderLabs said that locations of the victims is global (not the Netherlands).

SpiderLabs explained that they could not specify a targeted country because the attacker used a proxy server based in the Netherlands to push the outflow of traffic from an NL address (making it look like there are 1,049,879 victims in the Netherlands).

EVERNOTE PRODUCTS BUSINESS MARKET BLOGS

Security Notice: Service-wide Password Reset

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, changed or lost. We also have no evidence that any payment information for Evernote Premium or Evernote Business customers was accessed.

SynoLocker™

Automated Decryption Service

All important files on this NAS have been encrypted using strong cryptography

List of encrypted files available here.

Follow these simple steps if files recovery is needed:

1. Download and install Tor Browser.
2. Open Tor Browser and visit http://cypherxffttr7hho.onion. This link works **only** with the Tor Browser.
3. Login with your identification code to get further instructions on how to get a decryption key.
4. Your identification code is **19PYBCFK7UoR8PMhhoB8M4gwCPAPXUL3xr** (also visible here).
5. Follow the instructions on the decryption page once a valid decryption key has been acquired.

Technical details about the encryption process:

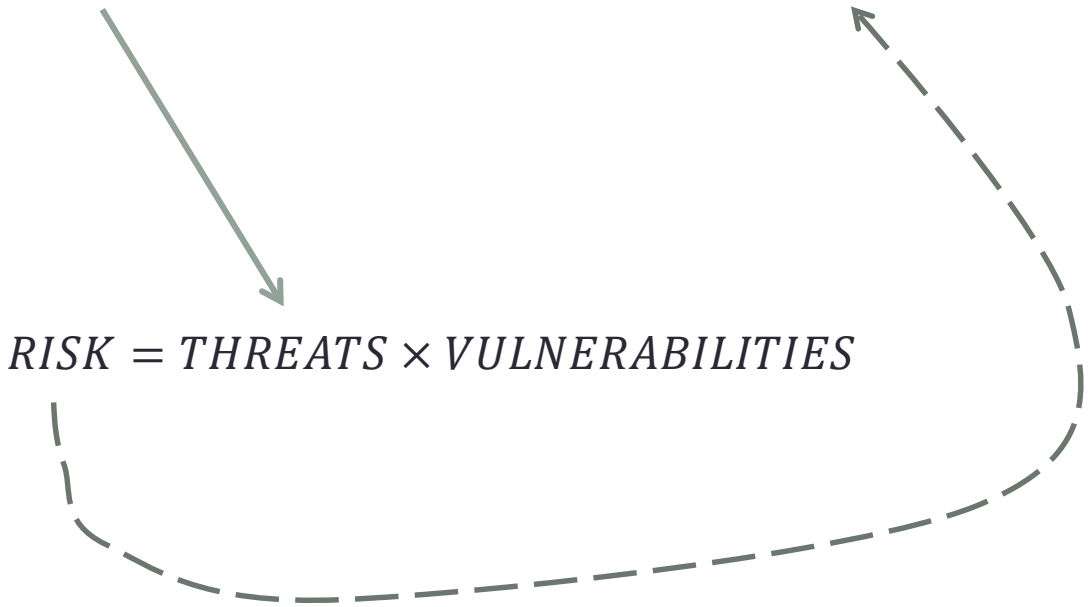
- A unique RSA-2048 keypair is generated on a remote server and linked to this system.
- The RSA-2048 public key is sent to this system while the private key stays in the remote server database.
- A random 256-bit key is generated on this system when a new file needs to be encrypted.
- This 256-bit key is then used to encrypt the file with AES-256 CBC symmetric cipher.
- The 256-bit key is then encrypted with the RSA-2048 public key.
- The resulting encrypted 256-bit key is then stored in the encrypted file and purged from system memory.
- The original unencrypted file is then overwrited with random bits before being deleted from the hard drive.
- The encrypted file is renamed to the original filename.
- To decrypt the file, the software needs the RSA-2048 private key attributed to this system from the remote server.

CVE-2013-4475, CVE-2013-6987

The dynamics of security

$$THREATS = ADVERSARIES \times REWARDS$$

$$RISK = THREATS \times VULNERABILITIES$$



Absolute Security?

- Eliminate design flaws
- Eliminate implementation bugs
- Add layers of security protection
- Eradicate the adversaries
- Decrease the reward

Three phases in achieving security

- Prevention
  - Formal verification, secure coding, fault tolerance design, law and regulations, manipulation of market, pay attention to human factors
- Detection
  - Detect violation of security policy
  - IDS, virus scanner, audit
- Response and Recovery
  - Stop attack, assess and repair damage, reconfigure
  - Fight back

Principles of secure system design

- Principle of adequate protection
  - Goal is not to maximize security, but to maximize utility while limiting risk to an acceptable level within reasonable cost
- Principle of effectiveness
  - mechanisms must be used properly, efficiently, and in a user-friendly manner

Principles of secure system design

- Principle of weakest link
- Principle of defense in depth
- Principle of least privilege
  - Each module (a process or a user) is only allowed access to information and resources that are necessary to its legitimate purposes
- Security by obscurity