

Operating System Security

Klaus Schütz
Windows OS Security
Microsoft Redmond

Before I start...

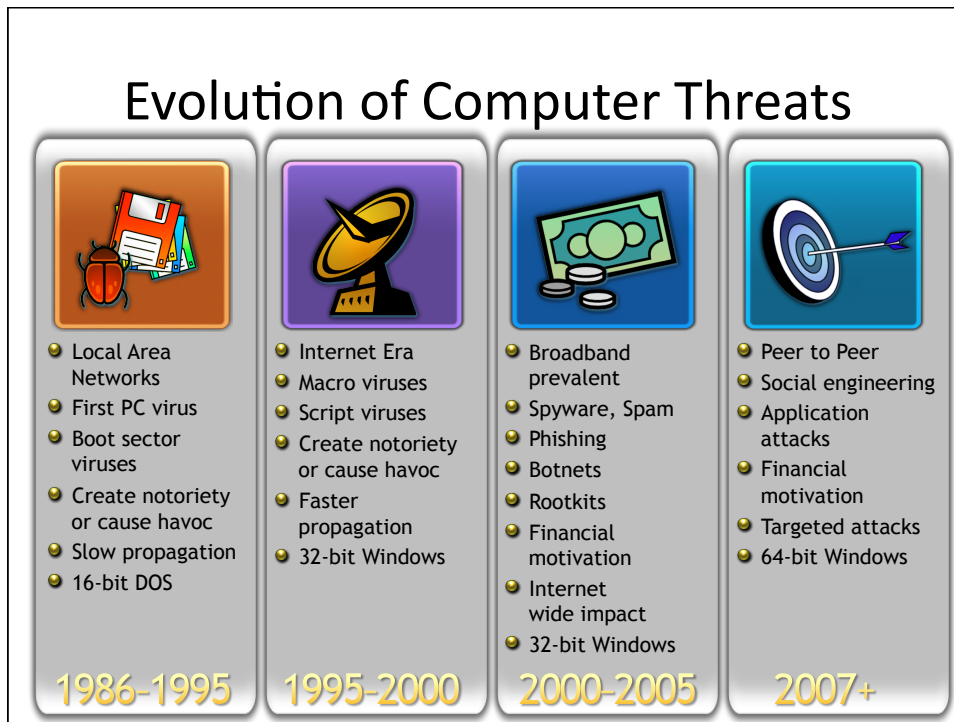
- My VP love(d) me
- A frustrated friend

Agenda

- Evolution of Threats
- Client vs. Server Security
- Operating System Security
- Software Development Lifecycle
- Take aways

What's in it for you?

- **Included**
 - Broad high level OS Security overview
 - Server AND Client Security
 - Things we (Microsoft) learned
 - Avoid getting burned
- **Not included**
 - Deep dive of any technology
 - Many pretty pictures



Today's Security Situation

- High public awareness of Security
- Broad use of computers
- Internet is great for committing crime
- Attacks happen in background
- Profits from crime are increasing

Addressing security challenges

Server vs. Client Security

Fundamental differences

1. Computer use

Server: HTTP, File, Database, Mail, etc

Client: Workstation, Laptop, Home Computer

2. Computer user

Server: IT Professionals (most of them)

Client: Everybody else

Server Security

- Security situation – simplified, of course
 - Network Location
 - Open Ports
 - Complex Configurations
 - OS and Application Bugs

It's easy to get it wrong

Server Security

- Addressing the Security situation
 - Change location
 - Packet inspecting firewall (e.g. ISA)
 - Configuration wizards (e.g. SCW)
 - Bare bones configuration
 - Well trained IT staff
 - Robust Operating System

Client Security

- Client Security Situation – again simplified
 - Changing location (e.g. laptop)
 - Many applications that want to ‘connect’
 - Users install almost everything
 - Users want ‘stuff’ to work
 - OS bugs
 - Many application bugs

Users want stuff to work

We will steal you credit card information, your private data and all the money in your account.
Do you want to continue?

Word failed to verify the integrity of the file ‘My PhD Thesis’. Do you want to open the file anyway?

Windows needs your permission to continue!

Client Security

- Addressing the Security situation
 - (That would be a talk on its own)
 - Robust Operating System

Robust Operating System

- Secure Platform - Overview
 - Isolation
 - Authentication
 - Access control
 - Code signing (drivers and applications)
 - Secure startup / TPM
 - Service hardening
 - Strong and modern cryptography
 - Malware protection
 - Software development lifecycle

Secure Platform - Isolation

- **Today**
 - User Mode / Kernel Mode Boundary
 - User to service isolation
 - User to user isolation
 - Levels of trust (IE)
- **Future**
 - Application isolation
- **Lessons learned**
 - System Windows pop up in session zero
 - IE protected mode

Secure Platform - Authentication

- **Credential types**
 - Username / password
 - Smart Cards / PKI
 - Cardspace
 - OTP / Tokens
- **Protocols**
 - Kerberos
 - NTLM
- **Lesson learned**
 - Use of blank passwords
 - Weak passwords
 - Default password policy
 - Smart Cards / PKI

Secure Platform - Access Control

- Access Control Lists – get ‘em right
- Network Access Protection (NAP)
- IPsec
- User Account Control (UAC)
- BitLocker

Secure Platform - Signing Drivers

- **The good stuff:**
 - Prevents loading of unsigned kernel code
 - Big impact on security
- **The challenge:**
 - Requires program for partners
 - Legal program
- **The bad stuff**
 - Does not prevent offline attacks
 - Does not always prevent rootkits

Secure Platform - Signing Applications

- **The good stuff:**
 - Prevents loading of unsigned user code
 - Big impact on security
- **The challenge:**
 - MANY unsigned applications
 - User experience
 - Legal program
- **The bad stuff**
 - Does not always prevent malware
 - I would not know that my VP loves me

Secure Platform - Secure Startup

- **The good stuff:**
 - Prevents offline attacks
 - Guarantees a 'clean' OS
- **The challenge:**
 - Requires hardware
 - Quite complex
 - Virtualization

Secure Platform - Service Hardening

- **The good stuff:**
 - 'Isolates' service
 - Limits or prevents access to network
 - Limits attack surface
- **The challenge:**
 - Still difficult to get it right
- **Lesson learned:**
 - Network access
 - Impersonation

Secure Platform - Malware Protection

- **Malware protection**
 - Windows Defender
 - IE Protected Mode
 - Windows Security Center
 - Address Space Layout Randomization
 - Data Execution Prevention

Software Development Lifecycle

- Ongoing training
- Attack surface review / threat modeling
- Expert reviews of designs
- Development Tools
- Security documentation
- Response plan
- Penetration testing
- Servicing

Attack Surface Review

- How will the application be used?
- Who are the users?
- From where does the data come?
- How does good data look like?
- How could bad data look like?
- How do you authenticate users?
- How do you control access?

Development Tools

- Programming language
- Compiler warnings (/W4)
- Stack overrun protection (/GS)
- Eliminate 'dangerous' APIs (strcpy)
- Prefast / prefix

Penetration Testing

- Throw 'junk' at APIs / Interfaces
- Use bad parameters
- Outside expert reviews
- Experts to pen test new software

Response Plan

- Expect bugs
- Have a contact point (e.g. MSRC)
- Designate a triage team
- Know the owner of the code
- Analyze and understand
- Come up with the right fix
- Know how to deploy
- Document and inform

Technology investments

- Tools
 - Compiler (e.g. /GS)
 - Scan for forbidden APIs (strecpy)
 - Prefast / Prefix

What we learned

- Security starts early in the design
- Good default settings
- Firewall on by default - Would have helped Todd
- Dis/allowed use of blank passwords
- Strong passwords for domains
- Smart Cards for secure access
- No use of Session Zero
- Restricted use of administrator
- Configuration wizards for server (SCW)

What we learned - continued

- Install and run as little as possible
- Avoid asking unnecessary questions
- If you have to make it really simple

Enhancing security - issues

- Application compatibility
- Usability
- Integration into existing deployments

Microsoft[®]
Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

