openHPI Course: Cyberthreats by Malware

Technical Failures

Prof. Dr. Christoph Meinel
Hasso Plattner Institute
University of Potsdam, Germany

Technical Failures as One of the Main Reasons for Malware Attacks

Malware needs an access point into any computer system. That could be:

- Human Factors → Next Video!
- **Technical Failures**

A technical failure is a deviation of the state of a computer system from its expected state

- Software design errors
- Software implementation errors
- Hardware errors
- Administrative errors (lack of knowledge / awareness)

Software Design Errors

Many software products are designed and developed without considering security aspects in depth!

- Software Developer ≠ Security Expert

Entire **Internet Protocol Suite** has been designed almost without security mechanisms

- IP, TCP, UDP …
- FTP & NFS transfer **passwords in plaintext!**
- TCP/IP cannot predict network nodes
  → **Network sniffing possible!**

Early Internet Standards RFCs explicitly stated that security concerns are not covered

Software Implementation Errors

Although the design of a software might be secure, the implementation can open holes for attacks:

- **Unchecked inputs**
- Missing fallback criteria (try, catch)
- Missing distinction between user groups, e.g. administrator vs. standard user
- Insecure cryptographic methods
- Hardcoded keys / passwords
- Hard-to-understand code
- (Test-) backdoors
- …

Hardware Errors & Failures

Substantial security risks from unreliable, unprotected or faulty hardware:

- **Design Errors of components**
- **Open ports** in the facility, e.g. USB, RJ45 …
- **Insecure reboot sequences** in case of power outage
- **Physically accessible devices**, e.g. Wifi router, switches, terminals, computers…
- …

Administrative Errors / Lack of Awareness

Administration errors are a common source for attacks

- **Default credential**, such as
  username: root, password: root
- Wrong domain settings
- Errors in the settings of firewall / IDS / IPS / SPAM filter / sandboxing environments…
- Unused standard **software** on computers
- Errors in networking, (reverse-) proxy, routing
- **Missing patches and updates** of old hardware and software
- Working with administrator / root accounts

Security Practices in Software Development

As errors and failures are wide-ranging, security precautions need to be taken

OWASP proposes **best security practices** for secure software development:

- Least privilege privileges (an application should only have as much access to resources as it needs)
- **Avoid security by obscurity**
- Keep security simple
- **Minimize attack surface** (delete unneeded programs)