

Phenoelit

meets

SIG<sup>2</sup>



# Introduction: whois phenoelit.de

- Phenoelit research areas
  - Protocol based attacks and exploitation
  - Embedded Systems exploitation
  - Design failures in products
- Phenoelit ethics
  - Vendor communication
  - No attacks on someone else's systems
  - The goal is raising awareness

# Dangerous believes I

- Trust in network level communication
  - Missing authentication
  - Trusting protocol level information
- Examples:
  - Protocols: RIP, IGRP, IRDP, ...
  - Cisco VPN Concentrator ISAKMP DoS
  - Cisco CDP and ICMP Redirect issues
  - Cisco TFTP long filename overflow

# Dangerous believes II

- Black box systems are more secure
  - Proved wrong: Cisco, HP, Nokia, etc.
- Embedded systems can not be exploited – only crashed
  - Proved wrong: IOS Exploit, HP Chai

# Dangerous practices

- Writing your own monolithic OS
  - Routers (Cisco, Lucent, D-Link, etc)
- Writing your own Web Server
  - 1001 Web Server products
  - Very few are secure
- Adding extensive functionality to the HTTP Protocol
  - Obfuscation still more used than crypto
  - HTTP misused as control and mgmt protocol

# Obfuscation Example

- HP Web JetAdmin password via HTTP  
6a206d14000a7c2bc3cd3358153cffb5
- Notice something?

6a206d14 = IV

000a = Length

7c2bc3cd3358153cffb5 = „code“

# Obfuscation Example

- HP Web JetAdmin password via HTTP decoding:

```
long v= IV;
for(int i=0;i<strlen(code);i++){
    v = 31413L * v + 13849L & -1L;
    code[i]=code[i]^(char)(1 >> 24);
}
```

# Discussion ...

- **Unprotected network infrastructure**
  - **Monolithic self-trusting code**
  - **Telnet(1) and HTTP management**
  - **Unencrypted & Unprotected protocols**
- **All these Web Servers**
  - **Common implementation flaws**
  - **Increasing Design flaws**
  - **False application of cryptography**

# Where is their stuff?

- <http://www.phenoelit.de>
- IRPAS – Routing protocol attacks
- Ultima Ratio – Cisco IOS Exploit
- Hijetter – HP Printer exploration
- VNCrack – sucks
- DPL – Default Account Database