

# **Mitigating An X.509 Flaw**

**Santosh Chokhani, Ph. D.**

# Briefing Contents

---

- **What the flaw is not**
- **What the flaw is**
- **X.509 Background**
- **Description of the Flaw**
- **Implications of the Flaw**
- **DSS Specifics**
- **Recommendations**



# What the Flaw is NOT

---

- **DSS is NOT broken**
- **FORTEZZA is NOT affected by the flaw**
- **MISSI PKI and Federal PKI are NOT affected by the flaw**



# What the Flaw is

---

- **Use of parameters in the issuer signature field and in the SIGNED MACRO field may be unsafe**
- **The above applies to both the certificates and the CRLs**



# X.509 Background

---

- **Both Certificate and CRL contain issuer signature field. The field contains the issuer algorithm object identifier. This field may optionally contain issuer public key parameters.**
- **Both Certificate and CRL SIGNED MACRO contain signature field. The field contains the issuer algorithm object identifier. This field may optionally contain issuer public key parameters.**



# Description of the Flaw

---

- The parameters in the four fields (2 in certificates and 2 in CRL) are vulnerable to substitution attack
- Attacker may replace the parameters (e.g.,  $p$ ,  $q$ ,  $g$  in the DSS) to translate a hard problem of computing a private key from public key and parameters to a new problem of computing a private from the real public key and substituted parameters
- The new problem may be easier or harder; it all depends on the cryptosystem



# Implications

---

- **Affects the trust in the entire PKI**
- **Attacker may create bogus certificates**
- **Attacker may create bogus CRL**



# DSS Specifics

---

- Attacker may select weak  $p$ ,  $q$ ,  $g$  to make the job of finding private key easier.
- A degenerate case consists of  $q = p-1$ ,  $h = g = y$ , and  $x = 1$ . This increases the signature size, but keeps it lower than  $q$ .
- DSS requires parameters to be obtained in authenticated manner. The values in the four fields are unauthenticated.
- DSS does not require signatures ( $r$ ,  $s$  each) to be 160 bits. It only requires signatures ( $r$ ,  $s$  each) to be  $< q$ . The simple attack meets this requirement.





# Recommendations

---

- **Ignore the parameters in the four field -- Easy to Implement**
- **Create an algorithm registry for DSS where parameters are “null” a la RSA and the subject public key syntax optionally contains parameters -- Most Secure in the Long Run; May Hinder Interoperability**
- **Make quality and size checks when using the parameters**
  - **Has performance implications**
  - **Is not a substitute for authenticated parameters**
  - **A comprehensive set of checks may not be practical**

