BULLRUN

[redacted]

PTD Lead for Special Operations and Policy

PTD "We penetrate targets' defences."

BULLRUN

- Covers the ability to defeat encryption used in specific network communications

- Includes multiple, extremely sensitive, sources and methods

PTD "We penetrate targets' defences."

Network Security Technologies

- Secure Sockets Layer/Transport Layer Security (SSL/TLS) (webmail)
- Secure Shell (SSH)
- Encrypted chat
- Virtual Private Networks (VPNs)
- Encrypted VoIP

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

PTD "We penetrate targets' defences."

Sensitivities

- Cryptanalytic capabilities
  - Are extremely difficult and costly to acquire
  - Require a long lead time
  - Depend on sensitive sources
  - Are very fragile
  - If lost, may never be regained
- The mere "fact of" a capability is very sensitive:
  - An adversary who knows *what* we can/cannot break is able to elude our capabilities even without knowing the technical details of *how* the capabilities work

PTD "We penetrate targets' defences."

Protecting BULLRUN Capabilities

- Technical and operational details
  - Need to be known only by cryptanalysts and those who enable cryptanalysis
  - Protected by established ECI's
    - PICARESQUE , PAWLEYS, AMBULANT, …
- "Fact of" information
  - Needs to be known very widely within the SIGINT production chain
  - Protect with new secure community of interest (COI)

PTD "We penetrate targets' defences."

Protecting the Info – Secure COI

- Secure Community of Interest (COI) – protects "fact of" as well as volume and scope of the capability
- BULLRUN indoctrination required for access to COI
- BULLRUN-related material, data – decrypted content and decrypted metadata, and details must be protected within the COI

Protecting the information

- BULLRUN is for internal (Sigint) use only
- Implemented at NSA &CSEC; DSD & GCSB to follow
- Not to be shared with UK Partners / customers
- EP not to reveal sources & methods; further guidance to be developed
- BULLRUN brief on Gcwiki for reference

Examples

- (S S1) Unspecified capabilities against [VPNs, IPSEC, TLS/SSL, HTTPS, SSH, PPTP, eChat, eVoIP]
- (TS S1 COMINT) Capabilities against the encryption used in [VPNs, IPSEC, TLS/SSL, HTTPS, SSH, PPTP, eChat, eVoIP]
- (TS S2 BULLRUN) Capability against specific applications

BULLRUN Bottom Line

- Groundbreaking capabilities
- Extremely fragile
- Do not ask about or speculate on sources or methods underpinning BULLRUN successes
- Indoctrination required for access to secure COI

PTD "We penetrate targets' defences."