ipfinity™
the CloudVoice™ company

Distributed Intrusion Detection and Prevention

The IPFINITY Methodology

A whitepaper on security, intrusion detection and prevention: the IPFINITY way

Methodology Overview

- All production software is widely-used and Open Source, or developed/modified in-house;
- All deployed software — including O/S components and kernel modules — is compiled from standard distributions from source code. No pre-compiled software is deployed;
- All O/S and application software components and major releases are tested for security, performance and ruggedness on non-production nodes before being promoted to production. Any indicated hardening is performed and tested prior to promotion. Logging verbosity is added or enhanced if required;
- Source code management is deployed to provide traceability of changes and change management

Methodology Overview

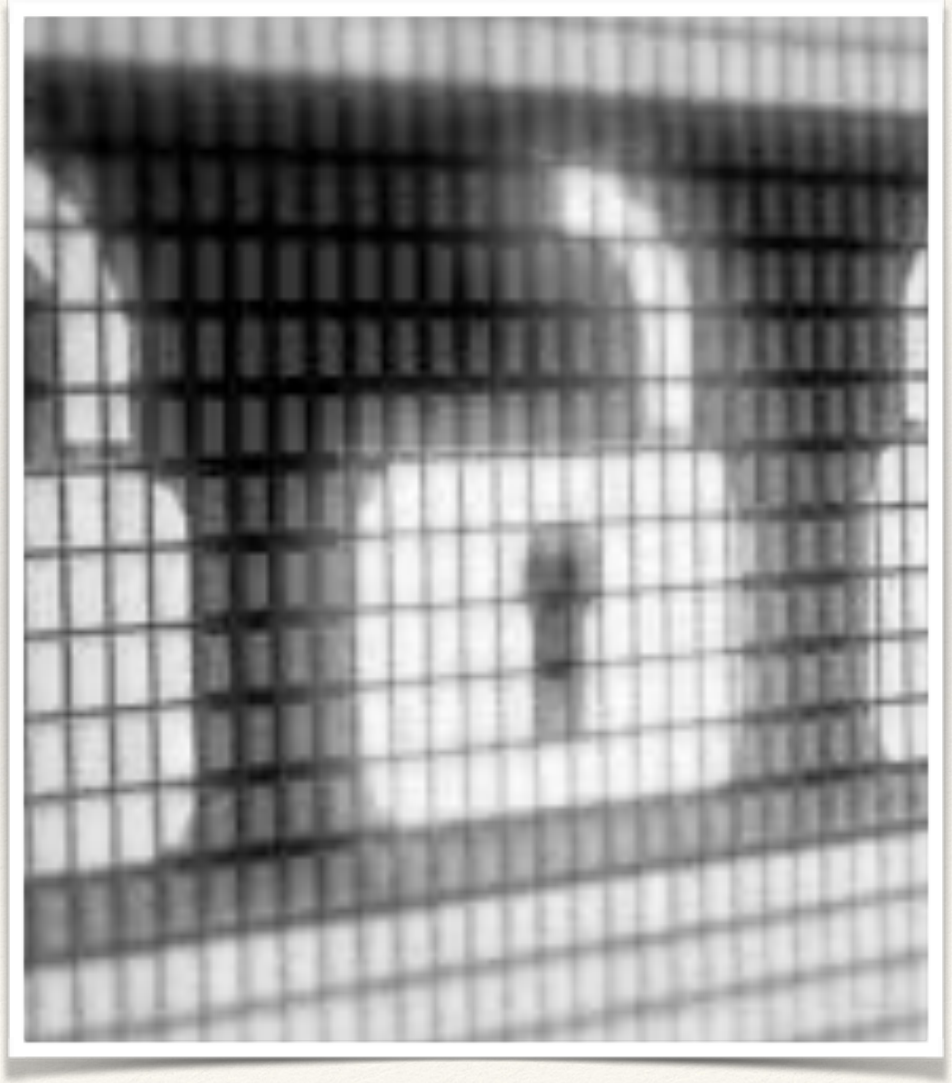
- Potential attack vectors are compiled from a first principles analysis as well as from the literature and the open source and security communities. IPFINITY's honeypots and public blacklists are used for capturing threat sources;
- Attack vectors are periodically tested against production nodes;
- System logs are periodically scanned by human operators to capture errors/anomalies that are not detected automatic scanners;
- Our automatic scanning suite, ibanx (developed by IPFINITY) is frequently updated to add rulesets;
- Ruleset and blacklist updates are *automatically distributed* to all nodes for NxN fanin/fanout.

Security of Credentials

- All systems' access is restricted by strong public-key cryptography (DSA/RSA); password access is explicitly disallowed for systems' access
- All customer access (e.g. SFTP) is via PKI (password access is disallowed)
- SHA1 hashes are utilized for key comparison
- Application software access is authenticated via SHA1 and source IP (if applicable)
- Private keys are never transmitted

Credential Provisioning/Injection

- SIP credentials are automatically generated during the provisioning process and are guaranteed hard;
- SIP credentials are only injected into production devices through a secure, automatic, "over the top" provisioning process and *never* transmitted in the clear;
- SIP credentials are regenerated and re-injected periodically.



Hardening

- Access is restricted to requires services (e.g. SIP, RTP, SSH or HTTP/HTTPS)
- Multi-factor authentication (MFA) is used for master authentication
- Auto-expiring and single-use credentials are used for short-duration and single-shot functions

Summary

- Distributed Intrusion Detection and Prevention requires an agile methodology that continuously adapts to the changing threat environment
- Code management, documentation, information sharing and adherence to the best cryptographic practices form the bulwark of IPFINITY's dIDP Protocol
- Vigilance and periodically reviewed, rigorous adherence to the dIDP Protocol contributes to the robustness of IPFINITY's dIDP practice

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand technology"

–Bruce Schneier

"There is no security panacea; only practice."

–Anonymous