Technology Differentiators

Technology Differentiators

Practically everyone in cyber-insecurity is essentially doing the same old things, deploying the same old technologies and getting the same old lack of results. Which is why we here at FN have thought about cyber-security very differently, radically differently in fact. In short, we examined and evaluated from first principles, the proverbial good, the bad and the otherwise of conventional wisdom as well as candidly many disregarded and discredited ideas that resonated with our worldview. **As such, the purpose of this paper is to provide context and composition to the core technologies that drive the FN Connect Secure Architecture of Security Agents and Ecosystem.**

1. FN Application Security Layer Protocol (ASL) Replaces SSL

The entire internet, including all/practically all security vendors rely on SSL for network security and given its numerous and well documented flaws, it's well known to be an insecure foundation to build upon…so we replaced it with a much more secure protocol, the FN ASL ~ Application Security Layer Protocol.

Secure Network Protocol

The FN ASL Protocol natively supports the protection of clients (resolvers) from forged DNS data and importantly insures the confidentiality of data, rendering attacks such Phishing, Pharming, DNS Poisoning et al completely ineffective(see BT Counterpane report) http://developfn.com/pdf/BT-Letter-of-Opinion-Federated-Networks-ASL-Protocol-November-2010.pdf. Additionally, vs. DNSSEC, FN's ASL Protocol scalably solves the backwards compatibility issue and is easier/less complex to implement. Further, the protocols ability to bind/"pair" tagged attributes such as passwords with URL's which along with bidirectional certificates and FN's trustworthy Trust Marks' play important roles in achieving the ASL protocol's material security enhancements vs. SSL.

Bi-Directional/Identity Aware

Bi-directional certificate implementation facilitates multi-directional access control, such that not only can the user validate a site, but the site can validate the User, which is of particular importance to login/authentication and ecommerce.

Digital 2nd Factor

The concurrent use of password and certificate based authentication creates a digital or virtualized 2nd factor authentication mechanism. In FN's implementation, even if an attacker was able to obtain a User's user name and password to a web application (i.e. through the "sticky note" attack or any other means), they still cannot login/impersonate the user. Obvious advantages include the lack of need for a second device and more importantly as related to security, device oriented 2nd factors are susceptible to Man-in-the-Middle attacks as well as easily hacked on a malicious host (i.e. key logging).

Zero Knowledge

Zero Knowledge protocols are one of the problems U.S. D.O.D. has listed as a "Hard Problem" as it requires that the privacy of a secret is not compromised in the process of providing its proof. The purpose of utilizing a Zero Knowledge implementation is to address the issue that User's are understandably uncomfortable with providing any central authority with access to their most important data, and was a central reason behind the backlash and subsequent failure of Microsoft Passport. Conversely, the FN ASL Protocol and it related services, such as FN's Authentic Attribute Authority enable the storage and validation of both User's and User data without ever providing FN with access to User data. (Note for greater clarity that this only applies to data fully protected by FN's ASL protocol).

Continued on next page

Least Privilege (Data Subset) Validation

Following the Principle of Least Privilege, under ASL a subset of certificate data attributes may be submitted to any validating party (vs. solely submitting full certificate data set for x509), with obvious security and privacy implications.

Extensible Data

Unlimited certificate attributes can be confidentially and securely stored and modified in real time (vs. small data set/"Walton's Mountain" problem and serious limitation of x509 certificates).

Real Time Update & Revoke

Certificate revocation, attribute addition/deletion or modification can be made dynamically, in real time (vs. x509 static updates).

2. Secure Human Computer Interface (Patent Filed)

Historically, a User's interaction with any digital system creates a vulnerable set of 'seams" for data leakage and thus a fertile ground for hacker exploitation. In stark contrast, FN's 'Identity Aware, Seamless, Extended End-2-End Reverse Sandbox' protects User data from the moment it is created to anywhere it may go as it traverses the Internet.

Diversified Cryptography

As part of FN's super encryption scheme, diversified cryptographic algorithms make digital input/output analysis and memory dumping materially more difficult.

Floating Virtual Keyboard

Specifically created to foil hardware key loggers and the statistical analysis of software input/output mechanisms.

Personalized, Un-detachable Symbol Augmented Trustmark's and Software Controls

Given the inherent bi-directionality of authentication, the user's authentication of the security software deployed is equally as important as the systems authentication of the user. Existing schemes typically either utilize a generic trust mark or some form of user defined 'mark' to denote the trust worthiness of websites and/or applications. Unlike existing trust mark schemes, FN's trust mark does not suffer from the obvious and critical security flaws related to either an inability to protect the symbols from Man-in-the-Middle attack and/or susceptibility to simple copying and subsequent deployment of forgeries (i.e. "spoofing"). Additionally, existing trust mark frameworks do not explicitly differentiate between the constructs of security and trust, nor do they enumerate and present a cogent trust, security and privacy ranking or "scaling" mechanism reflective of real world dynamics. Lastly, existing frameworks cannot easily be extended to include important non-security elements, such as organizational certifications and licensing (i.e. that a website/organization is a licensed charity, insurance company, etc.)

Continued on next page

3. Scheduled Updating/ Diversified Algorithms

By scheduling the aging/updating of our software we both reduce the time a hacker has to break FN's protection and creates a mechanism to facilitate the system "failing gracefully".
Diversified Algorithms make reverse engineering more difficult but also importantly change the economic or other reward potential of an exploit, from the "Break Once Break Everywhere" dynamic of today's homogenous algorithms towards the much less remunerative heterogeneous algorithm "Break |Once, Break Once" outcome.

Algorithm Diversification

Diversifying algorithms makes reverse engineering both more difficult and materially less remunerative, particularly when coupled with system integrity checking mechanisms.

4. Globally Scalable Identity

A secure digital identity systems that seamlessly integrates with e-government's multi- department and multi-jurisdictional aspirations, as well which scales globally.

User Centric

Enables a User, as the custodial owner of their data to not only control their data's security and privacy, but more importantly to actually be able to enforce their data sharing decisions.

Layered Validation

Existing authentication schemes are in fact merely self-asserted unique identifiers, having little to do with actual user identity. Again in stark contrast, FN's layered validation effectively scales the trust chain from users self-asserted and social trust mechanisms, to indirect 3rd party validation services (i.e. Equifax, Experian, etc.) and ultimately to actual Authentic Attribute Authorities, such as government institutions.

Authentic Attribute Authority (AAA)/ Networkable PKI

Outward facing and networkable, FN's Authentic Attribute Authority provides a "data-PKI" of sorts by facilitating a relying party's direct, zero knowledge validation of a claim, in real time (if need be), with the data attribute authority responsible for the attributes administration.

Zero Knowledge

All relying parties and network intermediaries will have no access to, or ability to compromise data. In fact, even the Authentic Attribute Authority's web enabled validation processes can operate on a zero knowledge basis (post its digital instantiation), effectively eliminating both external and internal (i.e. rogue employees) data threats to online data.

Bound/Tethered to Diversified Software and Hardware

FN affectively "registers" each software and hardware instance and binds/tethers each with the user's identity.

Continued on next page

Analog/Digital Domain Convergence

Existing system designs fail to concurrently incorporate user authentication and access requirements for both internet and non-internet use cases. For example, ID enabled smart cards cannot be used for internet authentication (unless smart card readers become built into computers, Smartphone's etc.).

5. Complimentary Enablers

Given the complexity and inherently 'all or none' dynamic of cyber security, a significantly large number of factors need to work concurrently and in a mutually reinforcing manner. As such, we view the following 'Complimentary Enablers' as necessary to the creation of materially more secure networked software, albeit not as potently or in as differentiated a manner as the items noted here-to-fore.

Fragilized

Code integrity guards/testers make dynamic analysis more difficult.

Hardware Binding

Although portable, FN client side software dynamically binds to a host system, making it more difficult for hacker's to try to break the software somewhere other than on the users host machine (and of course, hacking a User's software, while the user is using it, without them noticing…is also a more challenging exercise).

Tethered Services

Each FN client is tethered to a server and its services, making the actual use of exploited software much more difficult, most particularly for the multi-party use case which admittedly is perhaps most relevant to DRM. For instance, multi-users logging in concurrently with the same compromised FN client will be flagged to update the software, requiring it to be re-hacked and/or the FN server/service will simply instruct the hacked client(s) to fail.

Fail's Gracefully

If/when a fundamental component of the FN Secure Client Agent and/or Ecosystem fails, by design FN's scheduled updating capability can quickly and easily update all affected client software instances. For example, if RSA 2048 PKI encryption somehow becomes compromised, it can be replaced with an RSA Crypto with larger key size or any other form of proven algorithm, such as Elliptical Curve Cryptography, etc..

Fast Encryption

Part of a super encryption scheme intended primarily to make the capture of real data in memory more difficult (but admittedly not conceptually impossible).

Virtualized File System/ Secure Archive

All data at rest is encrypted by default and encryption is maintained irrespective of where the data is transferred to, or how (i.e. to USB, as an email attachment, etc.). Additionally, folder and file locations are more difficult for attackers to ascertain, providing materially enhanced protection vs. ransomware for any content created using an FN enabled Rich Text Editor.

Continued on next page

Secure/Maintainable Coding Practices
NASA Space Shuttle Code Maintainability Requirements

Does not eliminate OWASP type coding vulnerabilities, for FN's code base, but does reduce them. Most importantly however, when used in conjunction with fragilization, any potential vulnerability is much more difficult to exploit due the challenges associated with modifying code with integrity checking mechanisms.

Bitmaille™ Adhesive Security

FN's Bitmaille™ solution is a form of body armor for data, moving perimeter protection to the data level, enabling user centric/information centric security (i.e. conceptually moves the firewall from today's network or device perimeter to the application data level and explicitly binds user identity to data and both to the users software and hardware). Said another way, FN's cryptographic implementation begins much earlier in the data creation cycle, namely at the Human computer Interface and when combined with memory curtaining techniques, provides significantly enhanced data security.

End-2-End, No Seams

Seams or interfaces between components or systems provide fertile ground for data exploitation, a well known security issue associated with the assembly of best of breed point solution approaches (not to mention the cost and implementation challenges associated with same, but we digress…). In stark contrast, FN is 100% managed code from:

HCI ⇆ Client ⇆ Network Protocol ⇆ Server ⇆ Services

Autonomous Security as a Service

Providing a self-contained and self-reliant, seamless "end-2-end" solution stack materially reduces the security burden of all other networked software components, such as applications, browsers and operating systems and thereby materially reducing the transitive risk associated with the any other component(s). The important implication of this architectural outcome is the elimination of the "whack-a-mole" dynamic of both needing to keep up to date on the latest security flaw enumeration of the application "vulnerability de jour" and the subsequent fools errand of trying to patch multitudes of software instances on multitudes of devices.

Materially Reduced Attack Surfaces/"Easy Path is Mined"

Given the obvious inadequacies of anti-virus, intrusion detection and other environment "sterilization/cleanroom" approaches, the philosophy of FN's solution is instead analogous to "immunization". Succinctly, FN's Acute Threat Model assumes that all best of breed attack tools/threats reside concurrently on a malicious host with unpatched components (and can be operated combinatorially) and even in such a contrived malicious host threat model, the system must remain secure.

Sentient Factors (i.e. Multi-User Login)

For the most secure access control environments, multiple individuals (each with multi-factors to authenticate) are often required for authentication, such that the compromise of one person's authentication data and/or objects, including by coerced duress, cannot compromise the system.

Availability

User centric data back-up and dynamic/ real time cross domain restorability to any FN server enable high system survivability vs. natural or contrived denial of service scenarios.