National Cyber Leap Year Program Development Framework

Game Change Group-1:
Basing trust decisions on verified assertions (Digital Provenance)

What is the game change?

In today's game we have to expend considerable energy to discover whether to trust digital objects for any intended purpose. We are in the situation of a shopper who walks into the meat department of his grocery store and finds a case full of wrapped but unlabeled meat. While he might be able to determine if it is safe to eat through laborious chemical and microbiological analysis, some things he will never know: is it kosher; did the animals range free; what were they fed? Fortunately, USDA regulations ensure that each consumer does not have to invest in sophisticated laboratory equipment to analyze his beef, but in the digital world, this is often the very situation he finds himself in. Today, with no guarantees as to the source and integrity of digital content we have to check everything to be sure it is not harmful; with reliable digital provenance we can concentrate our resources instead on how we wish to handle the varieties of authorized content we receive.

What might this look like?

Filtering of all kinds becomes easier. Caller ID for email; application white-listing; authoritative patching; cyber IFF, anonymity-preserving credentials, adaptive trust policies

Why now?

Environment - While anonymity might have been one of the selling points of the early Internet, those who want to use it to make money or run an organization are beginning to clamor for the basic security guarantees fundamental to e-commerce. These are authenticity or provenance– where did the object come from, integrity or pedigree—is it what it says it is, and non-repudiation or attribution—who can be held accountable. The ability of malware, inadvertently invited in by a user, to install itself despite not being "authorized" is the most common attack vector today.

Technical - Many of the technical building blocks have appeared in some guise; cryptography seems to be the core enabler: mechanisms for signing and binding metadata to content; public key infrastructures; email directory constructs; digital rights management (DRM).

National Cyber Leap Year Program Development Framework

Game Change Group-2:
Crime doesn't pay (Cyber Economics)

What is the game change?

Today cyber-crime pays. So does cyber-espionage. These activities are attractive because the cost to engage in them is very small compared to the return on investment. Attack development costs can be amortized over both time and space. The cyber resources upon which the illicit activities are built are cheap, even free, thanks to webmail and botnets. Risk also is low when other people's assets are used to launch attacks. These advantages, however, may be more fragile than they look, as they are sensitive to slight perturbations in the economy of cost and exposure. In the new game we even the odds and make cyber malefactors take more risk at a lower rate of return.

What might this look like?

Theory of cyber risk markets, incentives, disincentives and value chains; market alignment; key value chain points where cost should be introduced; impact of immediate law enforcement at key points.

Why now?

Environment – Cyber crime losses are reaching intolerable levels
Technical – Advancements in attribution, forensics; better understanding of patterns of illicit actions and behaviors

National Cyber Leap Year Program Development Framework

Game Change Group-3:
Move from forensics to real-time diagnosis (Health-Inspired Network Defense)

What is the game change?

Today, weeks and months may elapse before successful network penetrations are detected through laborious forensic analysis. Despite their potential to function with intelligence, today's typical network components have very limited understanding of what passes through them, coupled with a correspondingly short memory. In medical terms, because we are not instrumenting for early detection of pathogens and their effects, our most common diagnoses are through autopsies of enterprises which have succumbed to attack. In the new game, network components have heightened ability to observe and record what is happening to and around them. With this new awareness of their health and safety they enjoy a range of options: they may take preventative measures, rejecting requests which do not fit the profile of what is good, *a priori*, for the network; they can build immunological responses to the malicious agents which they sense in real time; they may refine the evidence they capture for the pathologist, as a diagnosis of last resort, or to support the development of new prevention methods.

What might this look like?

Ability to automatically detect denial of service attacks; ability to find and stop propagation of botnets; ability to support user intent.

Why now?

Environment - With the spread of virtualized desktops and cloud computing, the network boundary itself is now virtual. Hardware switches and routers will increasingly utilize software mechanisms, completely opening up the previously ossified world of network protocols to redesign. There is room for both old and new protocols to co-exist.
Technical - ideas from the proposals; CleanSlate work.

National Cyber Leap Year Program Development Framework

Game Change Group-4:
Attacks only work once if at all (Moving-Target Defense)

What is the game change?

In the current game, attackers win by taking advantage of the relatively static nature of our systems. Adversaries can plan at their leisure, relatively safe in the assumption that our key IT assets will look the same for a long time. They can map out our likely responses and stockpile a set of exploits that escalates in sophistication as we deploy better defenses. They can afford to invest significant resources in their attacks because they expect to persist in our systems for a long time. In the new game we win by increasing the randomness or decreasing the predictability of our systems. By making the cyber terrain appear chaotic to the adversary, we force him to do reconnaissance and launch exploits anew for every desired penetration; the attacker enjoys no amortization of development costs.

What might this look like?

Non-persistent environments; randomized execution of code; utility computing decoupled from enterprise data assets; randomized network and host identities; randomizing compilers; dynamic address spaces; adopting new technology faster than bad guys can figure out flaws.

Why now?

Environment – Virtualization has moved from the server to the desktop, reducing start-up costs; multi-core processors are ubiquitous; cloud computing emerging; need to integrate new functionality faster than it can be secured

Technical – fault tolerance enabled by multiple cores; decade of experience with virtualization; hardware supports for virtualization in Intel chip set; mature research in avoiding memory-based attacks.

National Cyber Leap Year Program Development Framework

Game Change Group-5:
Knowing when we've been had (Hardware-Enabled Trust)

What is the game change?

One of the hardest things about today's game is not knowing when we're losing. Our trusty PC has no way to notify us that it has in fact become an enemy agent or a zombie, secretly exfiltrating our financial secrets to identity thieves, or spamming our neighbors for some botmaster. Since we have no real plan for checking and restoring the integrity of our assets once we start using them, we are forced into the impossible position of having to deploy impregnable systems. In the new game we persistently monitor our assets for changes in trustworthiness by embedding tamper-resistant roots of trust in the architecture. Attacks can be stopped in their tracks if we can isolate and decontaminate their host.

What might this look like?

Trusted boot; Trusted Platform Module (TPM)-enabled applications; measurement and attestation; integrity-breach alarms.

Why now?

Environment – Most modern PCs now have trusted execution chip set; root-kit detection is not very robust and the attack is commonplace; Trusted Computing Group (TCG) has wide set of members

Technical – TCG ideas are good and have government expertise inside; Intel has put a lot of work into the TPM and other hardware supports for trust; encouraging advancements in field-programmable gate arrays (FPGAs).