P | I | P | S

Securing the Next Biometric

Vulnerabilities of DNA-based Identity Verification Systems

PIPS White Paper 10.7: *Executive Summary*

Ranjani Parthasarathy, Research Fellow
Katherine Herthel, Research Intern

DNA will be the next biometric identifier, with wide-ranging applications from border security to rapid personnel identification. In the next decade, DNA sequencing may verify identities in near real time—minutes or even seconds. *DNA-based identity verification systems* (DIVS), however, have three major vulnerabilities. DNA-based biometric security is weakened by sale of private data from commercial genetic analysis, may be spoofed using DNA synthesis capabilities, and enables exploits using DNA-based malware. Current legislation inadequately safeguards US persons' genetic information. Further, open-access publications will proliferate DNA malware design and production capabilities. To protect the future viability of DIVS, policymakers will need to protect genetic information and review publication of sensitive biotechnology research.

DNA as the Next Biometric Authenticator

Global interest in biometric security is rising, yet current real-time biometrics, such as fingerprints and iris scans, cannot comprehensively differentiate between twins, relatives, or even unrelated individuals. DNA allows differentiation even between "identical" twins based on minimal differences in genetic sequence.

- *From Fingerprints to DNA.* Decreasing cost and increasing speed of DNA sequencing, in tandem, enable a probable future where DNA will be used as an effective biometric authenticator. Growing concerns about existing biometrics will likely accelerate a move towards DNA-based identity verification systems within the next decade.

- *The Road to DNA-based Identification.* A state-level reference DNA database is a prerequisite for DNA-based biometric security. Some states currently have national biometric databases or DNA databases for the explicit purpose of identification. Forensic databases on suspected or convicted criminals exist in 64 countries. Finally, DNA collection allows medical analysis, and is undertaken through Precision Medicine Initiatives that require broad DNA collection.

  Some DNA databases may also enable other outcomes: legal databases that target specific subsections of the population may speculatively enable the design of bioweapons tuned to individuals or ethnic groups. Additionally, the application of genetic analysis technologies

to exploiting DNA-based biometric security vulnerabilities may warrant additional scrutiny when such technologies in the hands of potential US adversaries.

Vulnerabilities of DNA-based Identity Verification Systems

Despite confidence in DNA as an authenticator, the capacity to develop workarounds or exploit future *DNA-based identity verification systems* (DIVS) poses a threat to US security. The United States faces three key vulnerabilities that will jeopardize the security of DIVS.

- *Commercialization of Genetic Information.* Through commercial offerings, private companies capture genetic data on US persons. These businesses then sell DNA sequence datasets to unknown end users, who may include foreign actors. Although nominally de-identified, the genetic sequences can be re-identified using other publicly available data, releasing genetic information whose security will be critical to implementing DIVS.

- *Synthesis and Spoofing.* Current trends in DNA synthesis technology will enable spoofing of a DIVS. Spoofing is defined as the presentation of a false identity to any authentication system. In the case of a DIVS, spoofing would take the form of one individual using another's DNA sequence. DNA synthesis technology may allow actors to spoof the DIVS using synthetic—artificial, biologically active—DNA.

- *DNA Malware.* Synthetic DNA sequences, in conjunction with poor network hygiene, can allow access to a secure network. DNA malware may be designed and used by states with resources in both cyberspace and biotechnology. Non-state actors may also be able to take advantage of this vulnerability using commercial synthesis techniques.

Current US Policy and Research Practices

Current US policy and research practices may accelerate the failure of DIVS, as US policies overlook security implications of genetic collection. Existing US federal policy regarding genetic data focuses on the medical implications of sequencing rather than future security applications—though a few US state laws offer stronger protections from a personal privacy standpoint. Further, previous US inaction following major national security leaks magnifies existing DIVS vulnerabilities. Compiling de-identified genetic data with previously publicized information about US national security employees or could rapidly accelerate the failure of DIVS by allowing more effective re-identification of DNA sequences. Finally, current US research into DNA-based malware is published with no review for national security applications, publicizing a DIVS vulnerability. Open-access publications on DNA malware will accelerate the proliferation of malware design and production capabilities.

Protecting Future Implementation of DIVS

Changes to US policy and research practices are required to preserve the opportunity for future US use of DIVS. In order to pursue a DNA-based identity verification system in the future, US policy

must more stringently monitor current data sales. Additional review of sensitive biotechnological topics, particularly DNA malware, will secure networks against DIVS as a weak point of entry. In addition, the United States must monitor the accessibility and cost of synthesis technologies in order to assess whether non-state actors have spoofing and malware capabilities and must also monitor states pursuing medical genomics.

Following appropriate changes in US policy, successful implementation of DIVS will improve security of physical facilities as well as network security. Pursuing DIVS may better secure the US border, but at the same time may pose challenges for safeguarding the identities of individuals—for instance, those who are part of witness protection programs. The implications of successful DIVS will ultimately lead to new policy challenges.